Secure Navigation and Authentication

LELAND STANFORD JUNIOR UNIVERSITY
DIE LUFT DER FREIHEIT WEHT
1891

Sherman Lo

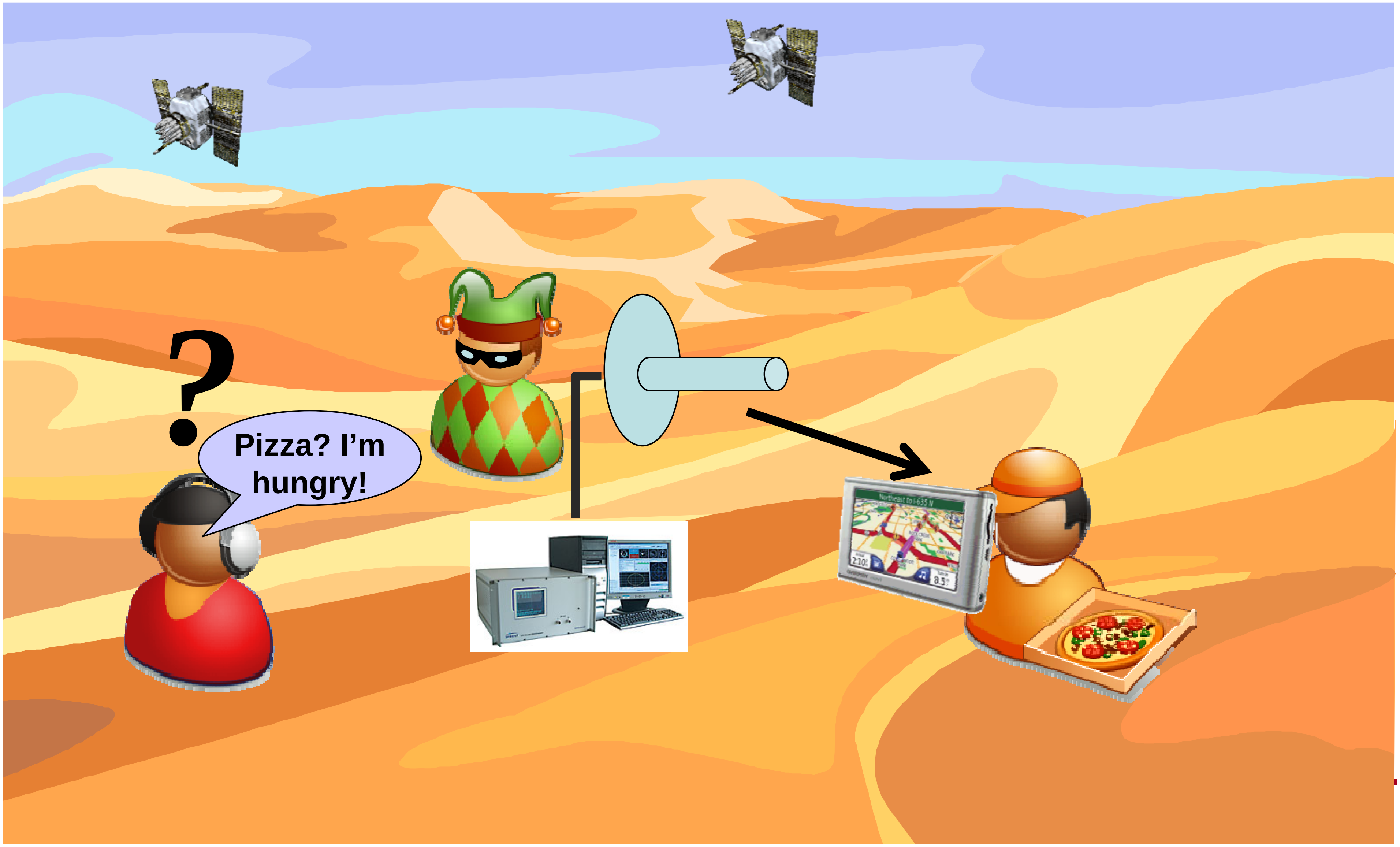
November 2008

Outline

- Motivating Authentication
- Proposed techniques for authentication
  - Source authentication
  - Cross checking
- My research

GNSS: Position, Navigation & Time

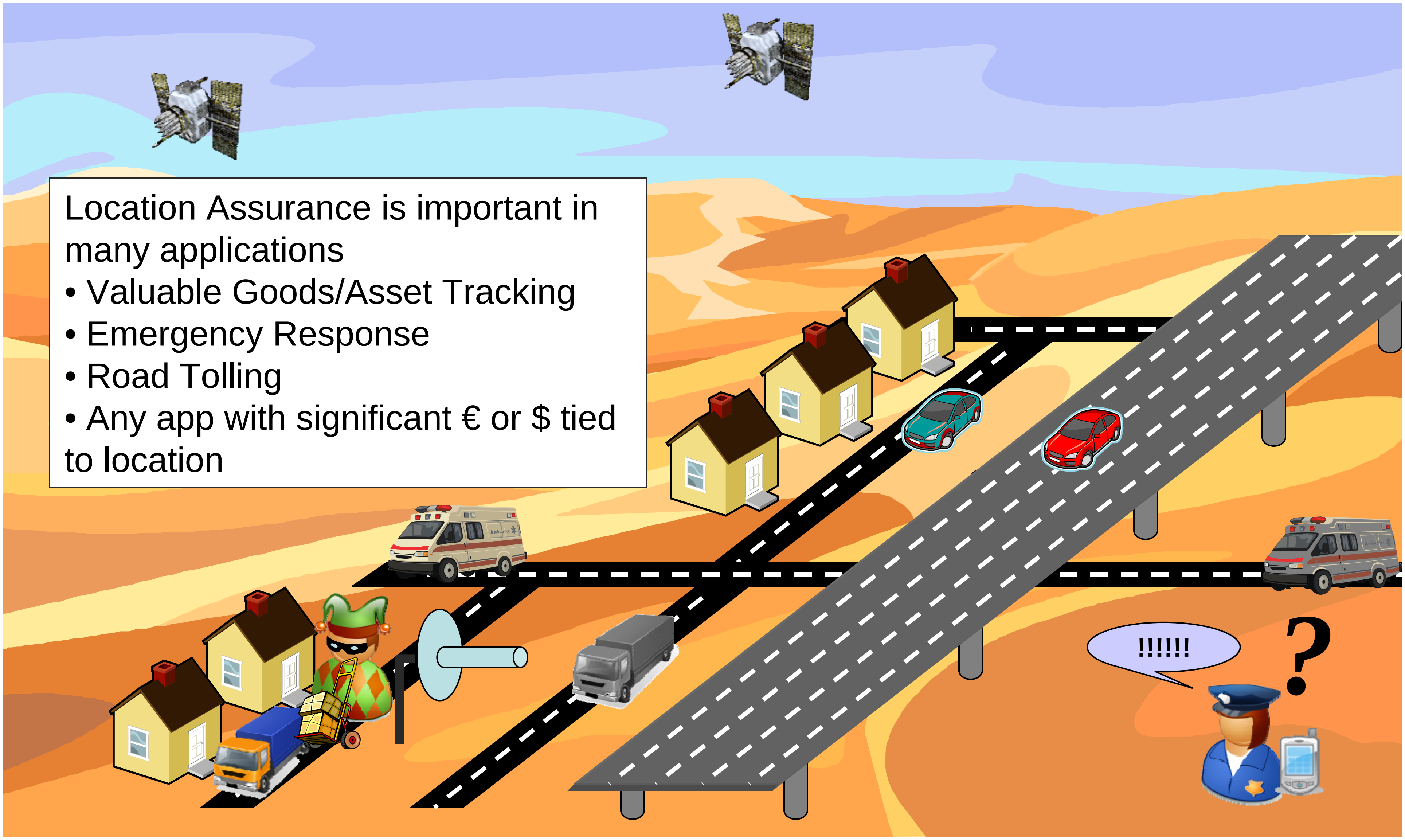
How do I know it is right?



Authentication: What is it & Why?

- GPS (and GNSS) being increasingly used for vital applications
  - Safety: aviation
  - Infrastructure: timing for cellular, power grid
  - Asset tracking & location
- Creates strong incentives to spoof
  - Reasons: Financial, Terrorism
  - Transport of valuable, dangerous material
  - Emergency response, geo fencing
  - Road tolls, taxi fare, & other financial transactions using navigation information
- Current civil signal easy to generate
- Authentication is the ability to verify the navigation signal’s source or content

Need for Location Assurance

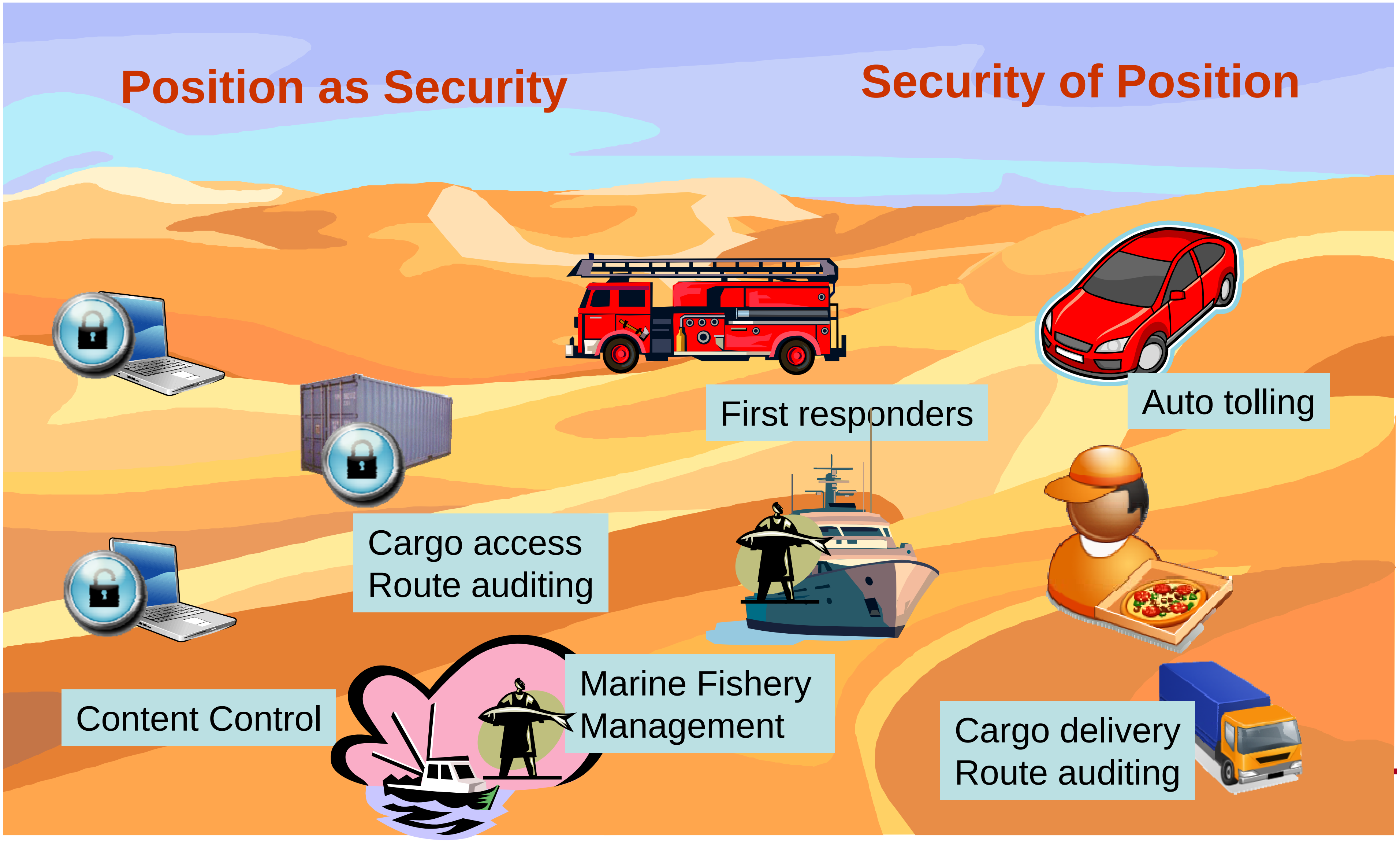


Location Assurance is important in many applications

- Valuable Goods/Asset Tracking
- Emergency Response
- Road Tolling
- Any app with significant € or $ tied to location

Incentive for Self Spoofing

GNSS (and Navigation) as a security tool



Position as Security

Security of Position

First responders

Auto tolling

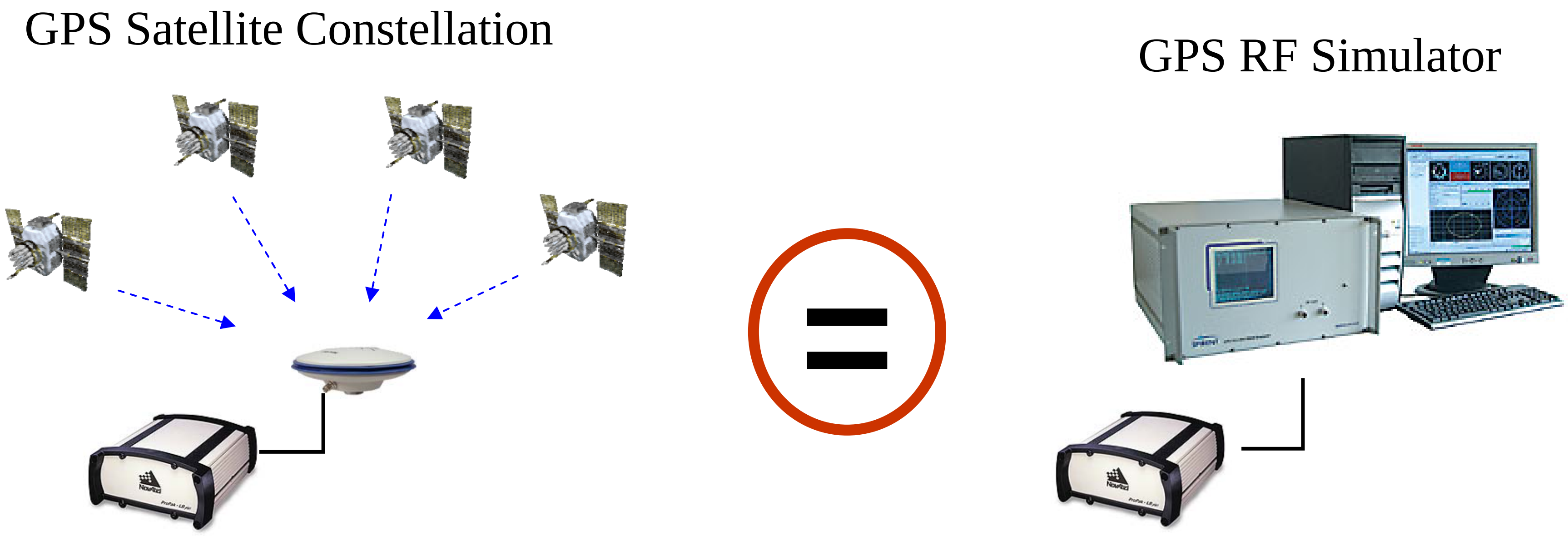
Cargo access
Route auditing

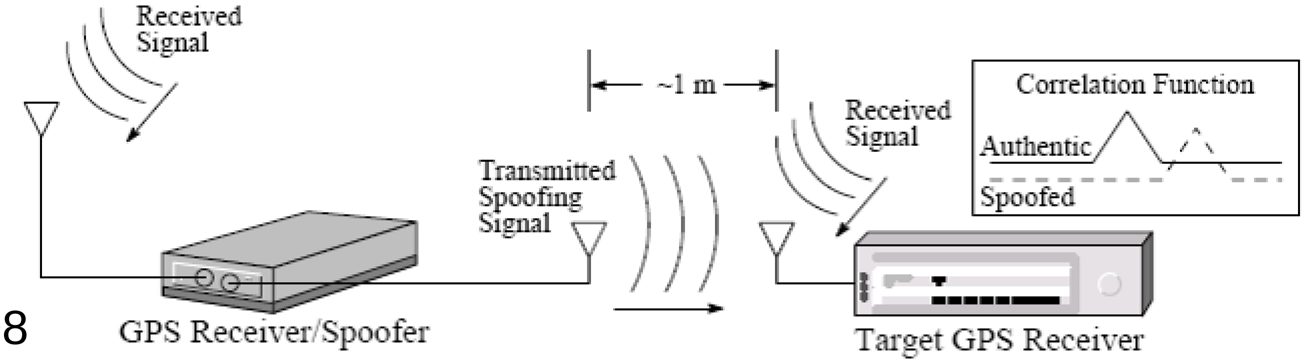
Content Control

Marine Fishery
Management

Cargo delivery
Route auditing

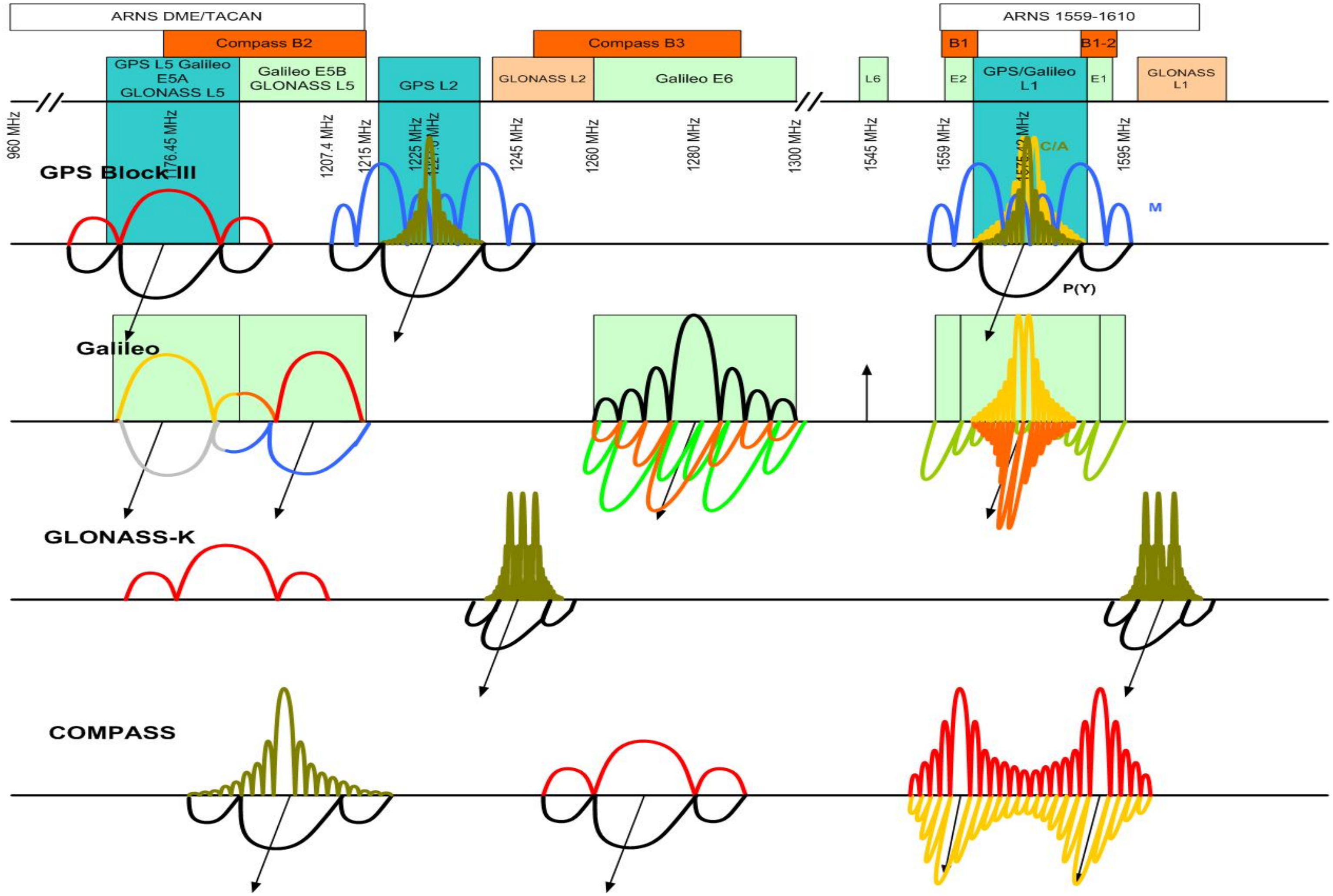
Spoofing civil GPS signals is quite feasible





Humphreys, IONGNSS 2008

Future Signals have Encryption for Restricted Users



Some Techniques

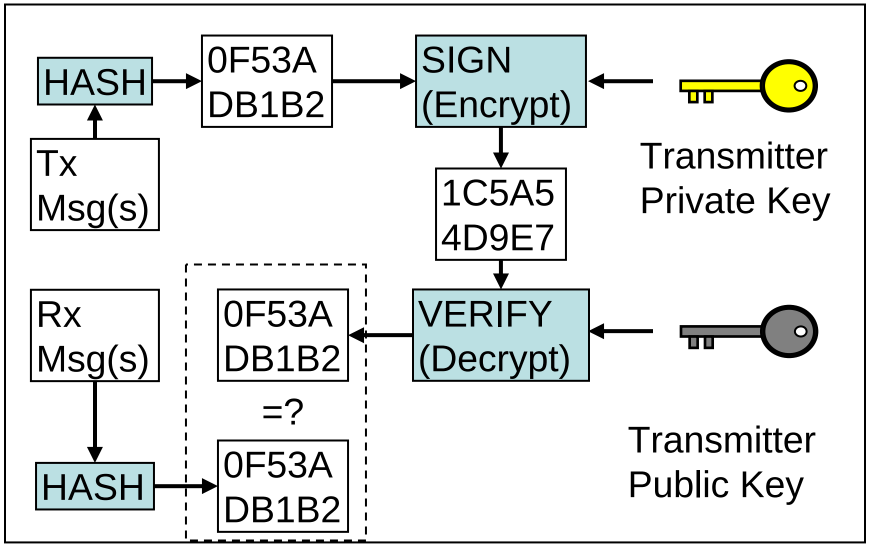
- 1. Data Authentication
  - Message contains “unforgeable” hash of information that verifies it has not been changed
  - Encryption key used to verify source
- 2. Public spreading code
  - Relies on GNSS signal below noise & difficult to extract
  - Delayed release of spreading code means not spoofable a priori/immediately
- 3. Private spreading code
  - Uses secret key that is never revealed
  - Requires secure receiver
- 1-3 still source data authentication
  - Verify source generated the info & that it has not been altered
  - Limit possible potential delay (hence spoofing)
- 4. Consistency checks of location related information

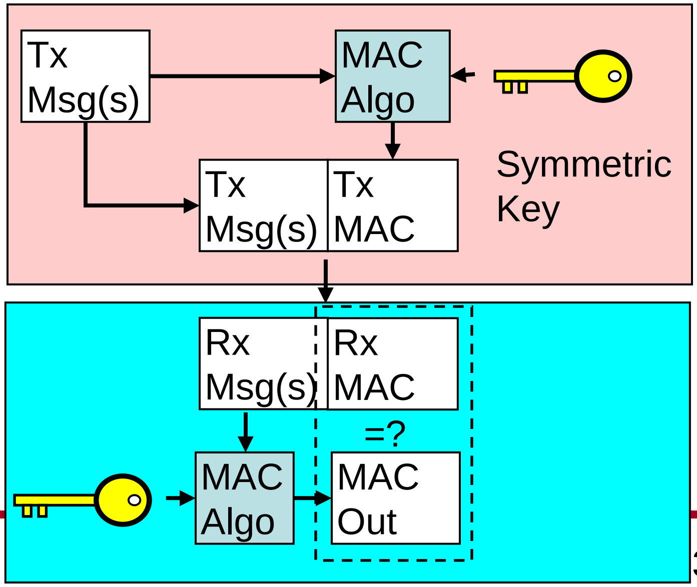
Classifying Proposed Techniques

- Hidden info revealed later
  - TESLA (symmetric key authentication)
  - Public Spreading Code
  - Requires some time synchronization
- Hidden info revealed never
  - Digital signatures (asymmetric key authentication)
  - Military service: W code, M code Galileo PRS
  - Private Spreading Code
  - Info hidden info for each sat cannot be extracted, no time sync is needed
- Position dependent properties
  - Different properties are observed at different locations (can determine this a priori)
  - May be possible but difficult

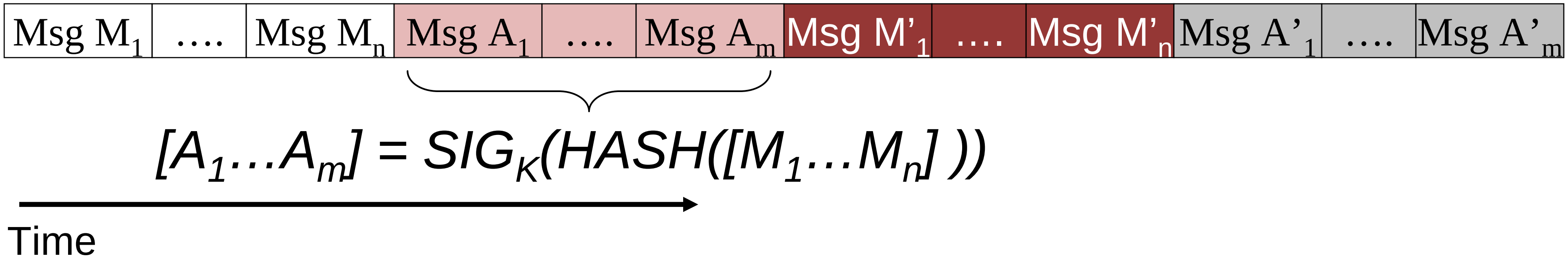
1. Data Authentication Techniques

- Digitally signed hash
  - Asymmetric key based
  - Private key signs hash
  - Validated by public key & msg hash
- MAC
  - Tag generated using msg and key
  - Difficult for attacker to generate valid msg, tag pair without key
  - Symmetric key is more efficient (data, computation)


HASH
0F53A DB1B2
SIGN (Encrypt)
Tx Msg(s)
Transmitter Private Key
1C5A5 4D9E7
Rx Msg(s)
0F53A DB1B2
VERIFY (Decrypt)
=?
Transmitter Public Key
HASH
0F53A DB1B2


Tx Msg(s)
MAC Algo
Tx Msg(s)
Tx MAC
Symmetric Key
Rx Msg(s)
Rx MAC
=?
MAC Algo
MAC Out

Signed Hash



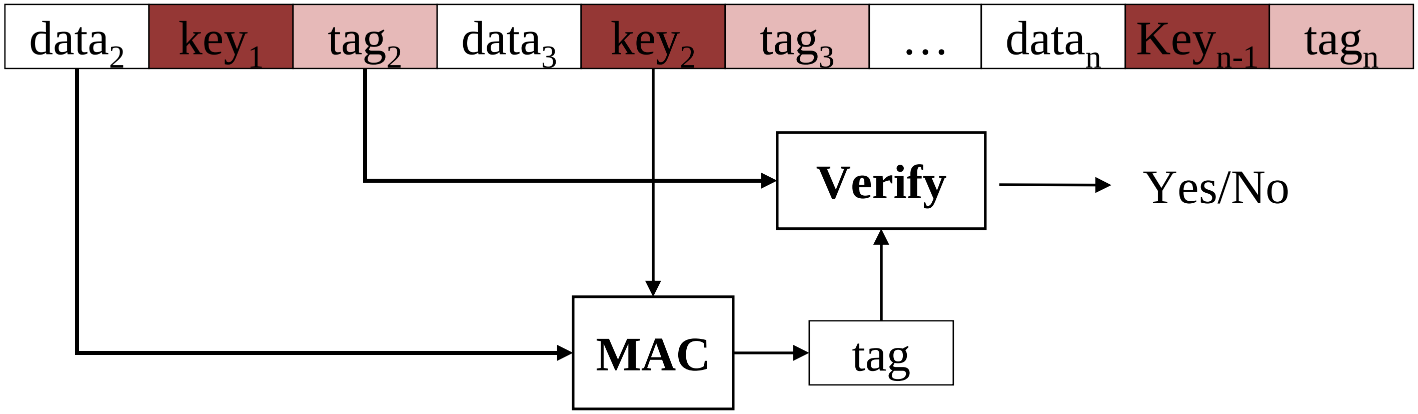
Msg M_1	….	Msg M_n	Msg A_1	….	Msg A_m	Msg M'_1	….	Msg M'_n	Msg A'_1	….	Msg A'_m

$$[A_1\ldots A_m] = SIG_K(HASH([M_1\ldots M_n]))$$

- Authentication accomplished by checking that the signed (with private key K) of hash of messages is correct
  - User has public key (requires key distribution)
  - With signature, data cannot be easily spoofed
- Delay is incurred
  - Must wait n+m messages to verify message M_1
- Elliptic Curve allows for greater data & computational efficiency

Basic TESLA

tag_m = MAC ($data_m$ key_m)



$data_2$	key_1	tag_2	$data_3$	key_2	tag_3	…	$data_n$	Key_{n-1}	tag_n

MAC

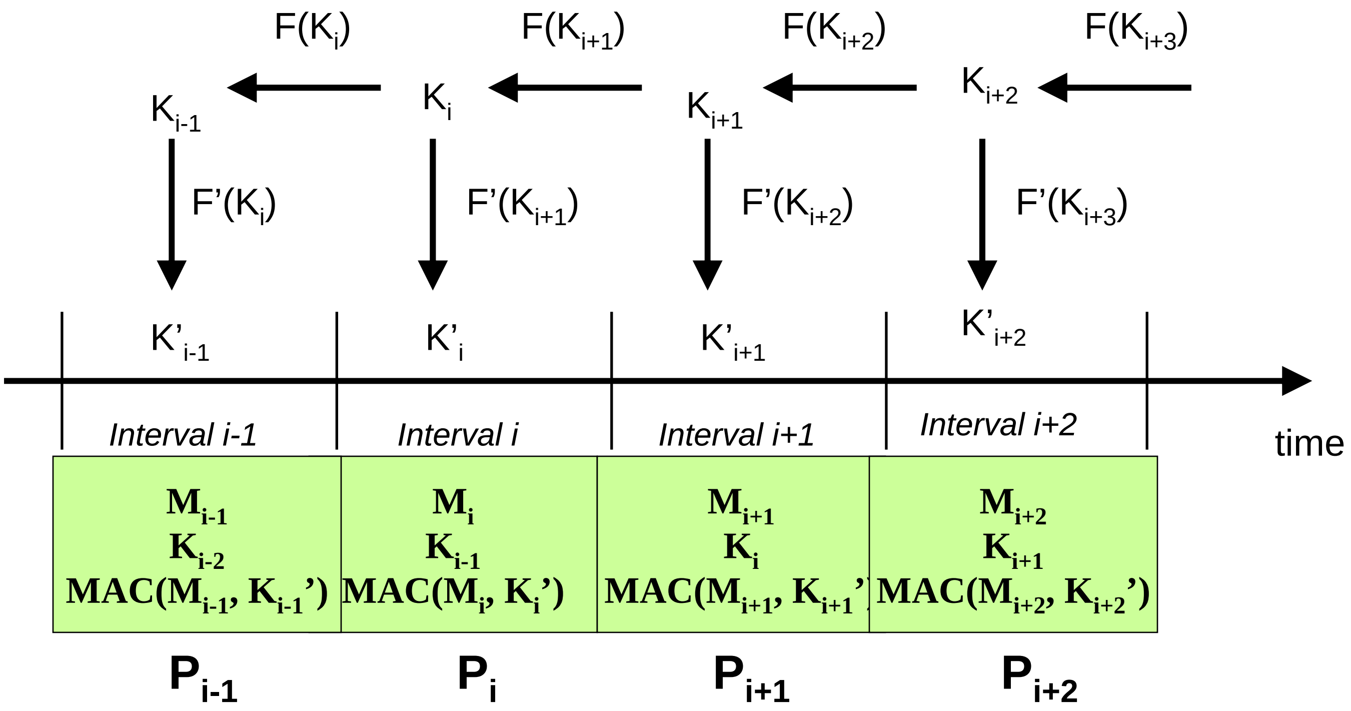
tag

Verify

Yes/No

- TESLA uses time (delayed key disclosure) to achieve the asymmetry property required for secure broadcast authentication
- Kuhn (2004), Wullems, et. al. (2005) proposed its use
  - Developed for networks
- Send data & hash, later reveal key to check that the data
  - Creates time window where spoofer cannot generate valid msg
- Key checked with based key using one way hash functions
  - If n hashes of key_n = base key, then key is from valid source

TESLA



- Pre-compute a sequence of key values using one-way hash functions or pseudo-random functions. $K_{n-1} = F(K_n)$, …, $K_1 = F(K_2)$
- Use another hash function to compute K’. $K_i' = F'(K_i)$
- Generate MAC using K’ and Message M
- Send packet P. $P_i = <M_i, K_{i-d}, MAC_i>$
- Distribute key K_0 via secure means (check K_i are from same source)

Authentication Strength and MAC Length

- Strength of authentication depends on choice of hash functions and bits used

Hash Function	Hash Length (bits)	Effective Strength (bits)	Time to break*
MD4	128	20	<1 sec
MD5	128	32	1 sec
SHA1	160	69	34 years
SHA256	256	128	10^{19} years

* $100K Hardware brute-force attack

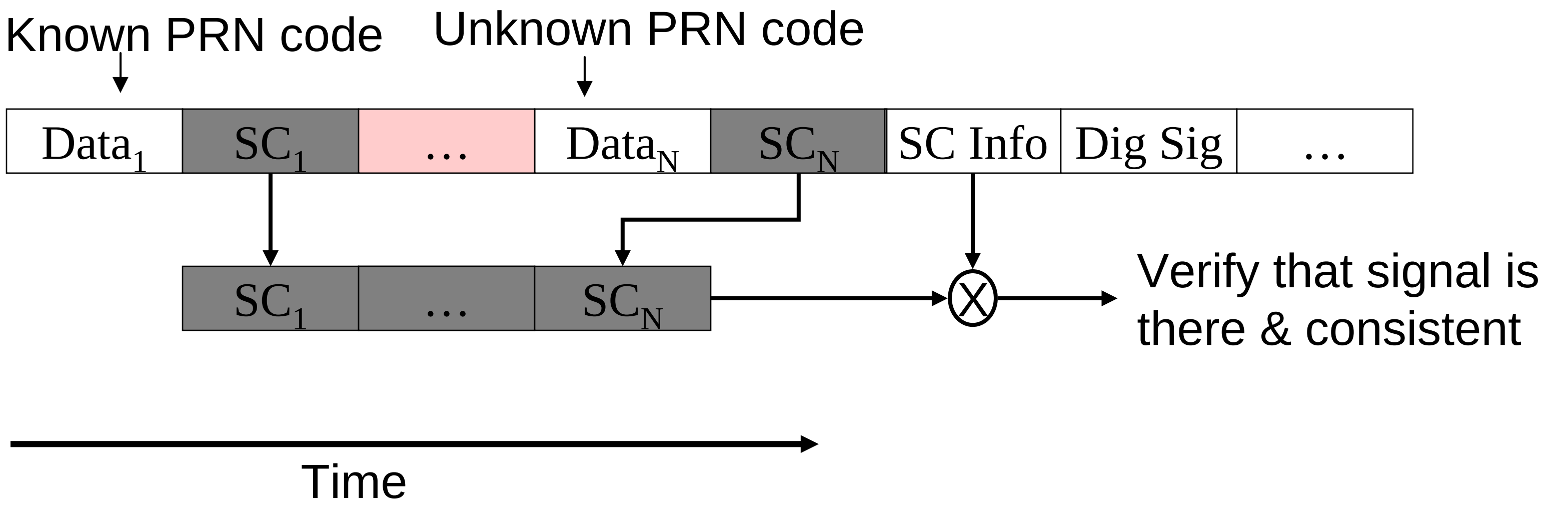
SHA 1 now 63 bits

Strength of MAC

Time from today (years)	Time to break SHA1	Time to break SHA256
0	34 years	10^{19} years
12	1.6 months	$4\text{x}10^{16}$ years
18	3 days	$2.4\text{x}10^{15}$ years
24	4.5 hrs	$1.5\text{x}10^{14}$ years

- Table of strength vs. time to crack above (give year) + Projection in 12 years (Moore’s law 2^8)
- Strength is limited by the length of the authentication data

2. Public Spreading Code



Known PRN code

Unknown PRN code

Data_1 | SC_1 | … | Data_N | SC_N | SC Info | Dig Sig | …

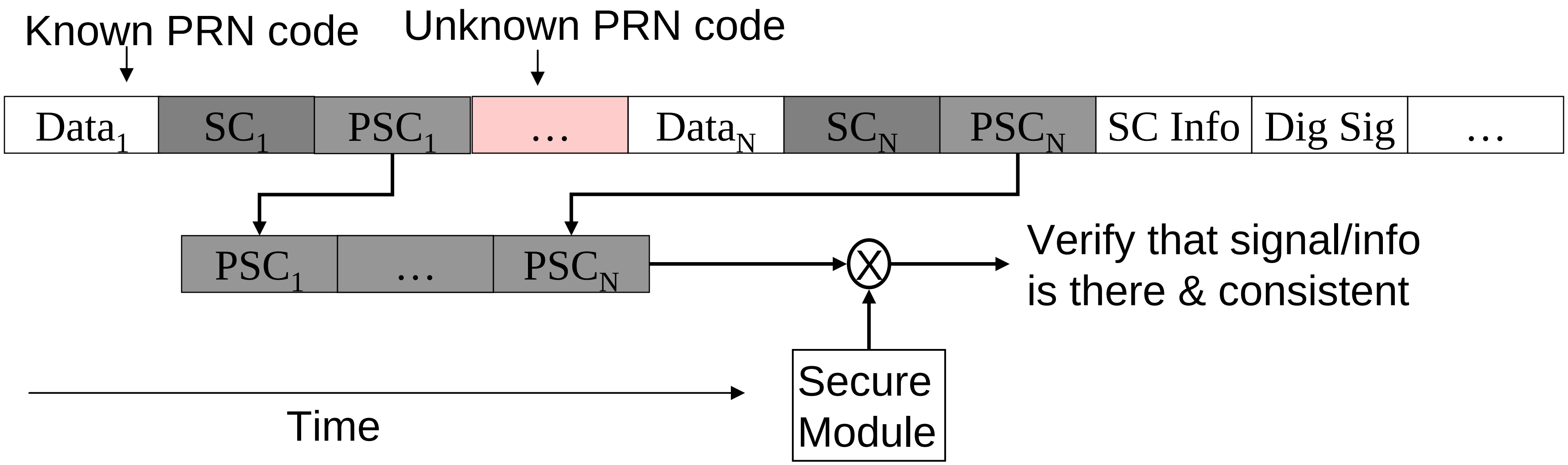
SC_1 | … | SC_N

Verify that signal is there & consistent

Time

- Scott (2003), Kuhn (2004)
- Spreading code segments stored until code revealed
  - Segments are transmitted at same time from each SV (overlap)
- Not spoofable until spreading code info is revealed
  - Time window dictates how synchronized the clock must be

3. Private Spreading Code



Known PRN code

Unknown PRN code

Data$_1$	SC$_1$	PSC$_1$	…	Data$_N$	SC$_N$	PSC$_N$	SC Info	Dig Sig	…

PSC$_1$	…	PSC$_N$

Verify that signal/info is there & consistent

Secure Module

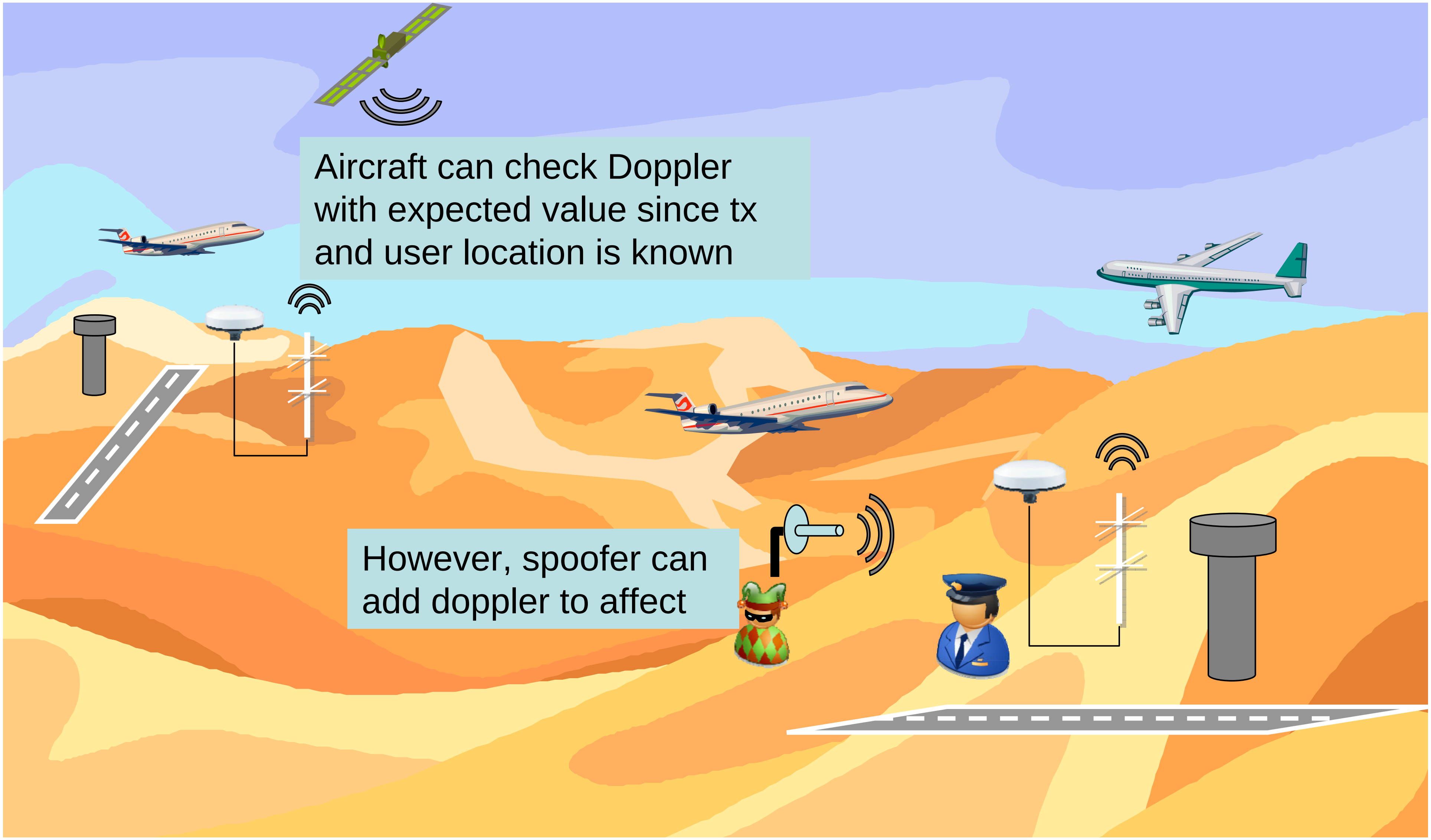
Time

- Similar to Military codes
- Implementation above is based on Scott (2003)
  - Limits some vulnerabilities of public spreading code but also retains some
  - Other ways to implement

4. Authentication through Information Consistency

- Doppler and other location measures
  - Difficult to spoof wide area & replicate
- Loran and other ground based nav systems have many other measures
- Multisystem measurements: GNSS, ground transmitters (DTV, Loran), INS, etc.

Consistency Checks Example: Doppler



Aircraft can check Doppler with expected value since tx and user location is known

However, spoofer can add doppler to affect

Current Civilian Authentication

- Constrain transmission
  - CAT II/III Requirements Development: Modifications to GBAS for VDB Authentication
    - Presented July 2008 by Tim Murphy
- Cross check measurements or info content
  - RAIM, AIME & other navigation related information
  - Checking consistency of measurements not spoofing

- Data authentication is still not common

Example: VDB Authentication Proposal

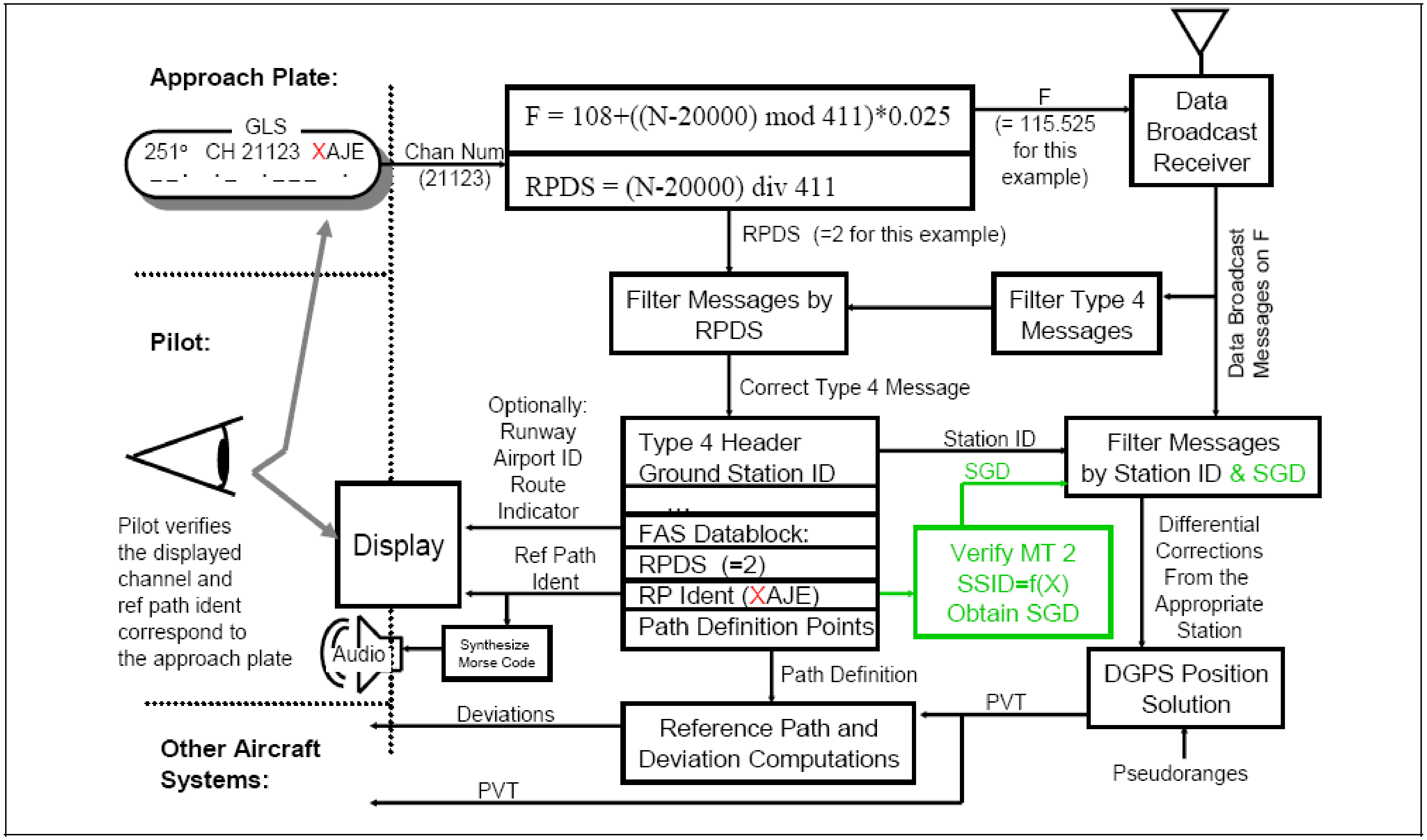


Figure 2 Approach Selection Scheme with the Proposed Authentication Protocols Added

VDB Authentication Goals

- Pilot identifies RPI (ref path id) – first char identifies 1 to 8 (SSID of gnd station) using Type 4 message matches approach plate
- Type 2 message give slot group def (SGP) which identifies slot of msg of the GS
  - Broadcast in the slot indicated by SSID

- Prevents spoofing to open slots
- Does not prevent overpowering GS or turning off GS and spoofing
  - If Type 4 or Type 2 msg hijacked, then spoofer can operate without interference

Securing Loran and Using Loran to Secure

GPS	Loran
Non-stationary satellites	Stationary transmitters
High absolute accuracy High repeatable accuracy	Low absolute accuracy High Repeatable accuracy
Global coverage	Northern hemisphere
Low SNR	High SNR
Easy to jam and spoof	Hard to jam and spoof
Indoor NOT capable	Indoor capable
Data channel	Data channel (e-Loran)

GPS Jammer

Thoughts

- Secure navigation info & authentication will become increasingly important
  - Navigation and GNSS becomes more important in economy and people’s lives
- Techniques do exist for authentication
  - Difficult to build into satellite
    - Must work easily within current infrastructure
  - Solution not requiring sat changes more likely/rapid
    - Receiver/ground based processing
    - Very possible to provide strong authentication
- With secure navigation, can use location to enable or strengthen various applications discussed
  - Valuable asset management, road tolling, emergency response, many others